

Towards composition of conformant systems

Houssam Abbas and Georgios Fainekos

Abstract—Motivated by the Model-Based Design process for Cyber-Physical Systems, we consider issues in conformance testing of systems. Conformance is a quantitative notion of similarity between the output trajectories of systems, which considers both temporal and spatial aspects of the outputs. Previous work developed algorithms for computing the conformance degree between two systems, and demonstrated how formal verification results for one system can be re-used for a system that is conformant to it. In this paper, we study the relation between conformance and a generalized approximate simulation relation for the class of Open Metric Transition Systems (OMTS). This allows us to prove a small-gain theorem for OMTS, which gives sufficient conditions under which the feedback interconnection of systems respects the conformance relation, thus allowing the building of more complex systems from conformant components.

I. INTRODUCTION

In Model-Based Design (MBD) of systems, an executable model of the system is developed early in the design process. This allows the verification engineers to conduct early testing [3]. The model is then refined iteratively and more details are added, e.g., initially ignored physical phenomena, time delays, etc. This eventually leads to the final model that gets implemented on some computational platform, for example via automatic code generation. See Fig. 1.

Each of the above transformations and calibrations introduces discrepancies between the output behavior of the original system (**the nominal system**) and the output behavior of the derived system (**the derived system**). These discrepancies are spatial (e.g., slightly different signal values in response to same stimulus, dropped samples, etc) and temporal (e.g., different timing characteristics of the outputs, out-of-order samples, delayed responses, etc) and their magnitude can vary as time progresses.

Ideally, the initial (simpler) model should be amenable to formal synthesis and verification methods (cycle 1 in Fig. 1) through tools like [5], [18]. To understand how the formal verification results on the simpler nominal model can be applied to the derived more complex system, it is necessary to quantify the *conformance degree* between them. The conformance degree, introduced in [1], [2], is a measure of both spatial and temporal differences between the output behaviors of two systems. It relaxes traditional notions of distance, like sup norm and approximate simulation, to

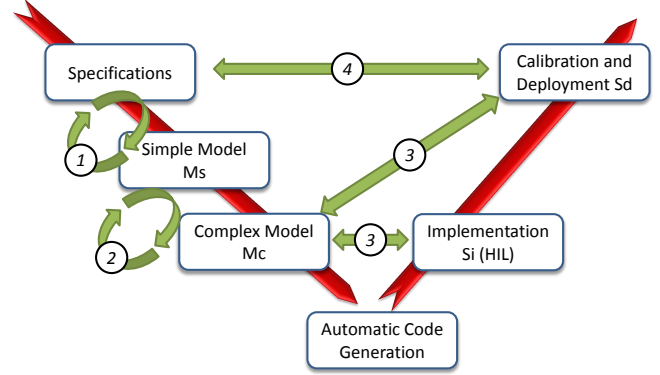


Fig. 1. Model-Based Development V-process.

encompass a larger class of systems, and to allow re-ordering of output signal values. In [2], it was shown how the formal properties satisfied by the derived system can be automatically obtained from knowledge of the properties satisfied by the nominal system, and knowledge of the conformance degree between them. In this paper, we extend that work by studying feedback interconnections of systems. Specifically, we are concerned with the following question: suppose we have a feedback interconnection of a plant and controller, and the closed-loop system has been formally verified to satisfy some properties. If the controller (or the plant) is replaced by another controller which is conformant to it, is the new closed-loop system conformant to the original closed-loop system? If yes, can we estimate its conformance degree without explicitly re-computing it? A positive answer to both questions would allow us to leverage the results in [2] and automatically deduce the properties satisfied by the new interconnection.

In this paper, we give a positive answer to both questions for a general class of dynamical systems modeled as *Open Metric Transition Systems* (OMTS). These are defined in Section II-A. The tool we use is a generalized notion of *Space-Time Approximate Simulation* (STAS) relation, which is defined in Section III-A. We show in Section III-B that the existence of such a relation between two OMTS implies that they are also conformant, and yields the conformance degree between them. In Section IV we provide a small-gain theorem for OMTS, which gives sufficient conditions under which feedback interconnections of OMTS respect approximate simulation, and therefore conformance. This is done via *STAS functions*, which are Lyapunov-like functions that certify the existence of a STAS relation between two systems.

H. Abbas is with the Department of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, U.S.A. hyabbas@asu.edu

G. Fainekos is with the School of Informatics, Decisions and Systems Engineering, Arizona State University, Tempe, U.S.A. gfaineko@asu.edu

This work was partially supported by NSF awards CNS 1350420 and CPS 1446730.

Notation. For a positive integer n , $[n] = \{1, \dots, n\}$. Given a set Σ , Σ^* is the set of finite strings on Σ , i.e. $\Sigma^* = \{s_0 s_1 \dots s_n \mid s_i \in \Sigma, n \in \mathbb{N}\}$. Given two sets A, B and $(a, b) \in A \times B$, $\text{pr}_A((a, b)) = a$.

II. CONFORMANCE OF OPEN METRIC TRANSITION SYSTEMS

In this section, we define a general system model, namely, Open Metric Transition Systems (OMTS). These extend Metric Transition Systems [8] in that they allow interconnection of systems, and will be our formalism of choice in this paper. We then define the conformance relations for OMTS and feedback interconnections for OMTS, which allows us to speak of controlled OMTS and compositionality in Section IV. As an illustration, we show how hybrid systems can be modeled as OMTS.

A. Open metric transition systems and conformance

A Metric Transition System (MTS) serves to model, at an abstract level, a fairly large class of systems. An MTS is a tuple $T = (Q, \Sigma_\chi, \rightarrow, Q^0, \Pi, \langle \rangle)$ where Q is a set known as the state space, $Q^0 \subset Q$ is the set of initial states, Σ_χ is the set of labels on which transitions take place, $\rightarrow \subset Q \times \Sigma_\chi \times Q$ is the transition relation, Π is the output set, and $\langle \rangle : Q \rightarrow \Pi$ is the output map. We write $q \xrightarrow{\sigma_\chi} q'$ to denote an element $(q, \sigma_\chi, q') \in \rightarrow$. Both Q and Π are metric spaces, that is, they are equipped with metrics d_Q and d_Π . Moreover, for any $q \in Q$ and any label subset $S \subset \Sigma_\chi$, the set

$$\text{Post}(q, S) = \cup_{\sigma_\chi \in S} \text{Post}(q, \sigma_\chi) \quad (1)$$

is compact in the metric-induced topology.

Given a string of labels $\bar{\sigma}_\chi = \sigma_{\chi,1} \sigma_{\chi,2} \dots \sigma_{\chi,m}$, we write $\bar{\sigma}_{\chi[i]} \in \Sigma_\chi^*$ for the prefix string $\sigma_{\chi,1} \sigma_{\chi,2} \dots \sigma_{\chi,i}$, $i \leq m$. The sets Σ_χ and Σ_χ^* are equipped with pseudo-metrics¹ d_{Σ_χ} and $d_{\Sigma_\chi^*}$, respectively, and Π is equipped with a metric d_Π . When two MTS share the same Σ_χ (Σ_χ^* , Π), they also share the same associated (pseudo-)metrics.

An Open Metric Transition System (OMTS) is a tuple $T = (Q, \Sigma, \rightarrow_T, Q^0, \Pi, \langle \rangle, p)$ where $(Q, \Sigma, \rightarrow_T, Q^0, \Pi, \langle \rangle)$ is an MTS as above. The label set Σ of an OMTS has a special structure: $\Sigma \subset \Sigma_u \times \Sigma_\chi$ for sets Σ_u, Σ_χ . The intuition behind this division is that Σ_u will be used to model input signals to the system embedded as an OMTS, and Σ_χ will be used to model the domain of that input signal. This departs from earlier approaches to embedding forced dynamical systems as MTS [7], because we need a way to describe interconnections of MTS, while preserving timing information in the interconnection. A generic label σ thus has two components: $\sigma = (\sigma_u, \sigma_\chi)$. The string prefix $\bar{\sigma}_{[i]}$ is defined similarly to the case of MTS. The *port map* $p : (\rightarrow_T) \rightarrow \Sigma \cup \{\nu\}$ associates a label to each transition in \rightarrow_T , or a special *empty label* ν . The empty label, as we will see, is used to allow a system to make empty transitions which don't change its state and don't advance time. The output of the port map will be used to compose OMTS.

¹A pseudo-metric does not separate points.

This makes them similar to hybrid I/O automata [14] but enriched with a metric structure, and with 'discrete actions' and 'trajectories of input variables' lumped into one label set, which fits well our usage of hybrid time.

We now define conformance between two OMTS T_1 and T_2 . Conformance quantifies the similarity between systems, and accounts for the fact that in a typical MBD process (Fig. 1), the output signals of the derived model will have temporal and spatial differences with the outputs of the nominal model. From the knowledge of the conformance degree between two systems, we can conclude what formal specifications are satisfied by one, given the specifications satisfied by the other [2].

Definition 2.1 (Conformance): Let T_1 and T_2 be two OMTS with a common output space Π and common label set Σ . Let τ, ε be two non-negative reals. Let $D \subset Q_1^0 \times Q_2^0$ be a relation defined on their initial sets. We refer to D as the *derivation relation*. We say T_2 **conforms to** T_1 **with precision** (τ, ε) **and derivation relation** D , which we write $T_1 \preceq_{\tau, \varepsilon}^D T_2$, if for all $(q_1^0, q_2^0) \in D$, and any sequence of T_1 transitions

$$q_1^0 \xrightarrow{\sigma_1} q_1^1 \xrightarrow{\sigma_2} q_1^2 \xrightarrow{\sigma_3} \dots \xrightarrow{\sigma_n} q_1^m$$

there exists a sequence of T_2 transitions

$$q_2^0 \xrightarrow{\alpha_1} q_2^1 \xrightarrow{\alpha_2} q_2^2 \xrightarrow{\alpha_3} \dots \xrightarrow{\alpha_n} q_2^{m'}$$

such that

- (a) for all $q_1^i, i \in [m]$, there exists q_2^k s.t. $d_\Pi(\langle q_1^i \rangle, \langle q_2^k \rangle) \leq \varepsilon$ and $d_{\Sigma^*}(\bar{\sigma}_{[i]}, \bar{\alpha}_{[k]}) \leq \tau$
- (b) for all $q_2^i, i \in [m']$, there exists q_1^k s.t. $d_\Pi(\langle q_1^k \rangle, \langle q_2^i \rangle) \leq \varepsilon$ and $d_{\Sigma^*}(\bar{\sigma}_{[k]}, \bar{\alpha}_{[i]}) \leq \tau$

Intuitively, the definition requires T_2 to be able to match any execution of T_1 , with some allowed deviation between the states that each execution visits, and some allowed deviation between the labels on which transitions take place. The matching is required not only for the final reached states q_1^m and $q_2^{m'}$, but for all intermediary states. The relation D is meant to capture the mapping between the initial states of one model (T_1) and the initial states of its implementation (T_2). For example, if T_2 is obtained by model order reduction from T_1 , D captures the reduction mapping as applied to the initial states. Because some of the labels in either transition sequence may be the empty label ν , more than one state in one sequence may match with the same state in the other sequence.

B. Feedback interconnection of OMTS

Given two OMTS T_1 and T_2 , we define their feedback interconnection as follows.

Definition 2.2 (Feedback in OMTS): Let T_i be an OMTS $(Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi_i, \langle \rangle_i, p_i)$, $i = 1, 2$, such that $\Sigma = \Sigma_u \times \Sigma_\chi$. Assume that $\Sigma \supset p_2(\rightarrow_2)$ and $\Sigma \supset p_1(\rightarrow_1)$. Their *feedback interconnection* is a (closed) MTS $(Q, \Sigma_{\chi 12}, \rightarrow, Q^0, \Pi, \langle \rangle)$, denoted $T_1 \circ T_2$, where

- $Q = Q_1 \times Q_2$
- $\Sigma_{\chi 12} \subset \Sigma_\chi$

- $Q^0 = Q_1^0 \times Q_2^0$
- $\Pi = \Pi_1 \times \Pi_2$
- $\langle (q_1, q_2) \rangle = (\langle q_1 \rangle_1, \langle q_2 \rangle_2)$
- $\rightarrow: (q_1, q_2) \xrightarrow{\sigma_\chi} (q'_1, q'_2)$ iff $\exists \sigma_1 = (\sigma_{1,u}, \sigma_\chi) \in \Sigma$ and $\sigma_2 = (\sigma_{2,u}, \sigma_\chi) \in \Sigma$ s.t. $q_1 \xrightarrow{\sigma_1} q'_1$, $q_2 \xrightarrow{\sigma_2} q'_2$, and $\sigma_1 = p_2(q_2 \xrightarrow{\sigma_2} q'_2)$, $\sigma_2 = p_1(q_1 \xrightarrow{\sigma_1} q'_1)$.

The output set distance is given by

$$d_\Pi((q_1, q_2), (q'_1, q'_2)) = \tilde{h}(d_{\Pi_1}(q_1, q'_1), d_{\Pi_2}(q_2, q'_2))$$

for some positive non-decreasing function \tilde{h} .

This is meant to model the situation when two hybrid systems are feedback interconnected, such that T_1 's outputs constitute the inputs to T_2 , and vice versa. Note that the definitions of output set, output map and associated distance function are somewhat arbitrary and ultimately depend on the application domain.

To simplify the statement of the main theorem and its proof, we introduce the following 'lifting' of $\Sigma_{\chi_{12}}$ to $\Sigma \times \Sigma$. The set Σ_{12} defined below contains all label pairs $(\sigma_1, \sigma_2) \in \Sigma_1 \times \Sigma_2$ allowed by the interconnection $T_1 \circ T_2$. Formally:

$$\begin{aligned} \Sigma_{12} := \{ & (\sigma_1, \sigma_2) \in \Sigma \times \Sigma \mid \sigma_1 = p_2(q_2 \xrightarrow{\sigma_2} q'_2), \\ & \sigma_2 = p_1(q_1 \xrightarrow{\sigma_1} q'_1), \sigma_{\chi_1} = \sigma_{\chi_2} \in \Sigma_{\chi_{12}}, \\ & \text{for some transitions } q_2 \xrightarrow{\sigma_2} q'_2 \text{ and } q_1 \xrightarrow{\sigma_1} q'_1 \} \end{aligned} \quad (2)$$

We note two properties of Σ_{12} :

- 1) $\Sigma_{12} \subset \Sigma \times \Sigma$
- 2) minimizing a function over the transitions enabled by labels in $\Sigma_{\chi_{12}}$ yields the same result as minimizing it over the transitions enabled by labels in the lifting Σ_{12} .

C. Problem formulation

The formal statement of this paper's problem follows:

Given two OMTS T_1 and T_2 connected in a feedback loop, and OMTS T_3 that conforms to T_1 with precision (τ, ε) and derivation relation D , is $T_3 \circ T_2$ conformant to the $T_1 \circ T_2$? If yes, what is the conformance degree between the two loops?

D. Embedding a hybrid system as an OMTS

Hybrid systems can be represented using, or embedded as, OMTS. This enables us to apply the compositionality result to them. We briefly define hybrid systems to show the embedding. Let C and D be subsets of \mathbb{R}^{n+m} , $U \subset \mathbb{R}^m$ be a set of input values, $F: \mathbb{R}^{n+m} \rightrightarrows \mathbb{R}^n$ and $G: \mathbb{R}^{n+m} \rightrightarrows \mathbb{R}^n$ be set-valued maps with $C \subset \text{dom} F$ and $D \subset \text{dom} G$. Let $z: \mathbb{R}^n \rightarrow \mathbb{R}^{n_z}$ be a function. The *hybrid dynamical system* \mathcal{H} with data (C, F, D, G, z) , internal state $x \in \mathbb{R}^n$ and output $y \in \mathbb{R}^{n_z}$ is governed by [10]

$$\mathcal{H} \begin{cases} \dot{x} & \in F(x, u) & (x, u) \in C \\ x^+ & \in G(x, u) & (x, u) \in D \\ y & = z(x) \end{cases} \quad (3)$$

The 'jump' map G models the change in system state at a mode change, or 'jump', and the jump set D captures the conditions causing a jump. The 'flow' map F models state

evolution away from jumps, while (x, u) is in the flow set C . System trajectories start from a specified set of initial conditions $H_0 \subset \text{pr}_{\mathbb{R}^n}(C \cup D)$. Finally, the output of the system y is given as a function z of its internal state, and its input is given by u which takes values in a set U .

Solutions (ϕ, u) to (3) are given by a hybrid arc ϕ and an *input arc* u sharing the same hybrid time domain $\text{dom} \phi = \text{dom} u$, and with standard properties that can be reviewed in [9, Ch. 2].

Definition 2.3 (Hybrid time domains and arcs [10]): A subset $E \subset \mathbb{R}_+ \times \mathbb{N}$ is a *compact hybrid time domain* if

$$E = \bigcup_{j=0}^{J-1} [t_j, t_{j+1}] \times \{j\}$$

for some finite increasing sequence of times $0 = t_0 \leq t_1 \leq t_2 \leq \dots \leq t_J$. A *hybrid arc* ϕ is a function supported over a hybrid time domain $\phi: E \rightarrow \mathbb{R}^n$, such that for every j , $\phi(\cdot, j)$ is locally absolutely continuous in t over $I_j = \{t : (t, j) \in E\}$; we call E the domain of ϕ and write it $\text{dom} \phi$.

A hybrid system $\mathcal{H} = (C, F, D, G, z)$ can be embedded as an OMTS $T = (Q, \Sigma, \rightarrow, Q^0, \Pi, \langle \cdot \rangle, p)$ as follows: $Q = \{x \in \mathbb{R}^n \mid \exists u : (x, u) \in C \cup D\}$, $Q^0 \subset Q$, $\langle \cdot \rangle = z$, and $\Pi = \mathbb{R}^{n_z}$. The label set is made of input arcs and their domains, and the empty label ν :

$$\Sigma = \{(u, \text{dom} u) \mid u \text{ is an input arc}\} \cup \{\nu\} \quad (4)$$

The transition relation is defined as $q \xrightarrow{\sigma} q'$ iff either $\sigma = \nu$ is the empty label and $q = q'$, or $\sigma = (u, \text{dom} u)$ and there exists a solution pair (ϕ, u) s.t. $\phi(0, 0) = q$, $\phi(t, j) = q'$ for some (t, j) in $\text{dom} u$. The port map p is defined as

$$p(q \xrightarrow{\sigma} q') = \begin{cases} (z(q), (0, 0)) & \text{if } \sigma = \nu \\ (z \circ \phi, \text{dom} \phi) & \text{otherwise} \end{cases}$$

where (ϕ, u) is the solution pair of \mathcal{H} corresponding to σ as defined above in (4).

Later in the paper, we will need to impose a requirement on d_Σ , namely, equation (5) from Section III-B. The rest of this section shows how d_Σ can be defined so this requirement is met. First, given an input arc u with domain E and two subsets $E' \subset E$, $E'' \subset E$ such that $(0, 0) \in E' \cap E''$ and $\sup_j E' = \sup_j E''$, the restrictions of u to E' and E'' respectively are said to have a common extension. (So the restricted arcs start at $(0, 0)$ and make the same number of jumps).

Let $\sigma = (u, E)$, $\sigma' = (u', E')$ be two labels with $E = \bigcup_{j=0}^{J-1} I_j \times \{j\}$, $E' = \bigcup_{j=0}^{J'-1} I'_j \times \{j\}$ compact hybrid time domains with J and J' jumps, respectively. Define

$$d_\Sigma(\sigma, \sigma') := \begin{cases} \max_j d_H(I_j, I'_j) & \text{u and u' have a} \\ & \text{common extension} \\ \infty & \text{otherwise} \end{cases}$$

Here, d_H is the symmetric Hausdorff distance between two sets. A string $s = \sigma_1 \sigma_2 \dots \sigma_m$ is then a concatenation of the

input arcs and their hybrid time domains², and is itself a valid pair (input arc, hybrid time domain). That is, in this case, $\Sigma^* \subset \Sigma$. Therefore given two strings s and a , we simply define $d_{\Sigma^*}(s, a) = d_{\Sigma}(s, a)$. It can be shown that this satisfies (5).

III. FROM SIMULATION RELATIONS TO CONFORMANCE RELATIONS

A. Space-Time Approximate Simulations

A *Space-Time Approximate Simulation* (STAS) relation is an approximate simulation relation in the sense of [12]. We choose to introduce the new terminology in order to avoid potentially awkward (and possibly confusing) references to ‘simulation relations in the sense of [xyz]’. STAS were introduced in [12] and applied in [13] to the study of networked control systems.

Our interest in this paper is on conformance as defined earlier, which is a notion defined on entire trajectories. STAS relations, defined on individual states of systems, is a related notion which has the advantage of having a functional characterization, much like Lyapunov functions characterize stability. In this section, we define STAS relations and connect them to conformance. The functional characterization of STAS can then be used to characterize conformance.

Definition 3.1 (STAS): Given two OMTS $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle \cdot \rangle_i, p_i)$, $i = 1, 2$, and positive reals τ, ε , consider a relation $R \subset Q_1 \times Q_2$, and the following three conditions:

- 1) $\forall (q_1, q_2) \in R, d_{\Pi}(\langle q_1 \rangle, \langle q_2 \rangle) \leq \varepsilon$
- 2) $\forall (q_1, q_2) \in R, \forall q_1 \xrightarrow{\sigma_1 \in \Sigma} q'_1, \exists \sigma_2 \in B_{\tau}(\sigma_1)$ and a transition $q_2 \xrightarrow{\sigma_2} q'_2$ s.t. $(q'_1, q'_2) \in R$
- 3) $\forall q_1^0 \in Q_1^0, \exists q_2^0 \in Q_2^0$ s.t. $(q_1^0, q_2^0) \in R$

where $B_{\tau}(\sigma) = \{\sigma' \in \Sigma \mid d_{\Sigma}(\sigma, \sigma') \leq \tau\}$. If R satisfies the first 2 conditions, then it is a (τ, ε) -**space-time approximate simulation** (STAS) of T_1 by T_2 . If in addition it satisfies the third, then we say T_2 **simulates** T_1 **with precision** (τ, ε) .

STAS relations describe what happens when T_1 ‘plays’ label σ_1 , and T_2 is allowed to respond by playing a label from $B_{\tau}(\sigma_1)$. In particular, it says that T_2 can always find a label such that the distance between the reached outputs is less than ε . In the rest of this paper, we will often simply speak of a simulation to mean a STAS.

B. From simulation to conformance

The connection between STAS, which is a relation between states, and conformance, which is a relation between executions, is captured in the following proposition.

Proposition 3.1: Given two OMTS $T_i = (Q_i, \Sigma, \rightarrow_i, \Pi, \langle \cdot \rangle_i, g_i)$, $i = 1, 2$, let R be a (τ, ε) -STAS relation between them, and let $D \subset Q_1^0 \times Q_2^0$ be a derivation relation between

²The concatenation of two compact hybrid time domains $E = \bigcup_{j=0}^{J_1-1} ([t_j, t_{j+1}] \times j)$ and $E' = \bigcup_{j=0}^{J_2-1} ([t'_j, t'_{j+1}] \times j)$ is the hybrid time domain $E_c = \bigcup_{j=0}^{J_1-1} ([t_j, t_{j+1}] \times j) \cup \bigcup_{j=0}^{J_2-1} ([t'_j + t_{J_1}, t'_{j+1} + t_{J_1}] \times \{j' + N_1\})$

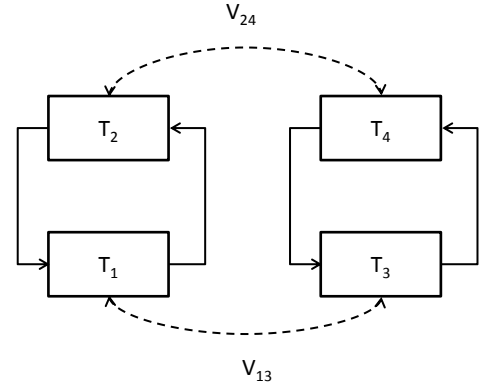


Fig. 2. Interconnections of similar MTS

them. Assume that the label pseudo-metrics d_{Σ}, d_{Σ^*} are such that for any two strings $\bar{\sigma} = \sigma_1 \dots \sigma_i$ and $\bar{\alpha} = \alpha_1 \dots \alpha_i$,

$$(\forall k \leq i, d_{\Sigma}(\sigma_k, \alpha_k) \leq \tau) \implies d_{\Sigma^*}(\bar{\sigma}_{[i]}, \bar{\alpha}_{[i]}) \leq \tau \quad (5)$$

If $D \subset R$, then T_2 conforms to T_1 with precision (τ, ε) and with derivation relation D . \square

Proof: Take any pair $(q_1^0, q_2^0) \in D$, and any sequence of T_1 transitions

$$q_1^0 \xrightarrow{\sigma_1} q_1^1 \xrightarrow{\sigma_2} q_1^2 \xrightarrow{\sigma_3} \dots \xrightarrow{\sigma_n} q_1^n$$

Because $D \subset R$, there exists a T_2 transition $q_2^0 \xrightarrow{\alpha_1} q_2^1$ s.t. $\alpha_1 \in B_{\tau}(\sigma_1)$ and $(q_1^1, q_2^1) \in R$, therefore $d_{\Pi}(\langle q_1^1 \rangle, \langle q_2^1 \rangle) \leq \varepsilon$. Proceeding in this way for every $k \leq n$, we build a sequence \mathbf{q}_2 of T_2 transitions

$$\mathbf{q}_2 = q_2^0 \xrightarrow{\alpha_1} q_2^1 \xrightarrow{\alpha_2} q_2^2 \xrightarrow{\dots} \dots \xrightarrow{\alpha_n} q_2^n$$

such that $d_{\Sigma}(\sigma_k, \alpha_k) \leq \tau$ and $d_{\Pi}(\langle q_1^k \rangle, \langle q_2^k \rangle) \leq \varepsilon$ for all k .

Now we check condition (a) of Def.2.1. For any $q_1^i, i \leq n$, $d_{\Pi}(\langle q_1^i \rangle, \langle q_2^i \rangle) \leq \varepsilon$ and by property (5) of the label pseudo-metric, $d_{\Sigma^*}(\sigma_{[i]}, \alpha_{[i]}) \leq \tau$. Thus condition (a) is satisfied. By construction of the execution \mathbf{q}_2 and symmetry of d_{Π} and d_{Σ} , we also have condition (b). \blacksquare

IV. COMPOSITIONALITY

In this section, we prove a general small gain condition under which the feedback interconnection of OMTS preserves similarity relations. By Prop. 3.1, this implies that conformance is also preserved under these conditions. We work in the OMTS formalism as it bypasses unnecessary technicalities and allows us to establish the result in greater generality, while maintaining continuity with the work of [13].

A. Compositionality of similar metric transition systems

Consider OMTS T_1, T_2, T_3, T_4 with label sets $\Sigma_1 = \Sigma_2$ and $\Sigma_3 = \Sigma_4$. Systems T_1 and T_2 are feedback interconnected to yield $T_1 \circ T_2$, with state space $Q_{12} = Q_1 \times Q_2$, and label set $\Sigma_{\chi_{12}}$. Similarly, systems T_3 and T_4 are feedback interconnected to yield $T_3 \circ T_4$, with state space $Q_{34} = Q_3 \times Q_4$, and label set $\Sigma_{\chi_{34}}$. See Fig. 2. We seek conditions under which $T_3 \circ T_4$ simulates $T_1 \circ T_2$; based on Prop.3.1, this would

imply that under the same conditions, $T_1 \circ T_2 \preceq_{\tau, \varepsilon}^C T_3 \circ T_4$ for some (τ, ε) . To do so, we use the functional characterization of STAS.

Definition 4.1: [12, Def. 3.2] Given two OMTS T_1 and T_2 with common output set Π and label set Σ , and non-negative real τ , a function $V : Q_1 \times Q_2 \rightarrow \mathbb{R}_+ \cup \{\infty\}$ is a τ -**simulation function of T_1 by T_2** if for all $(q_1, q_2) \in Q_1 \times Q_2$,

$$\begin{aligned} \text{A0)} \quad & V(q_1, q_2) \geq d_\Pi(\langle q_1 \rangle, \langle q_2 \rangle) \\ \text{A1)} \quad & V(q_1, q_2) \geq \sup_{q_1 \xrightarrow{\sigma \in \Sigma} q'_1} \inf_{q_2 \xrightarrow{\sigma' \in B_\tau(\sigma)} q'_2} V(q'_1, q'_2) \end{aligned}$$

A τ -simulation function defines a (τ, ε) -STAS relation via its level sets. Namely, as shown in [12, Thm. 3.4], the ε -sublevel set of V

$$\mathcal{L}_\varepsilon^V = \{(q, q') \in Q_1 \times Q_2 \mid V(q, q') \leq \varepsilon\} \quad (6)$$

is a (τ, ε) -STAS relation of T_1 by T_2 for all $\varepsilon \geq 0$.

To keep the equations readable, in what follows, we define the following: given $\sigma_{12} = (\sigma_1, \sigma_2) \in \Sigma_{12}$,

$$B_\tau^{34}(\sigma_{12}) := \{(\sigma_3, \sigma_4) \in \Sigma_{34} \mid d_{\Sigma_X}(\sigma_{\chi_1}, \sigma_{\chi_3}) \leq \tau\}$$

(Σ_{34} is defined analogously to Σ_{12} in (4)). The ball $B_\tau^{34}(\sigma_{12})$ contains all labels in Σ_{34} whose ‘chronological component’ σ_{χ_3} is no more than τ -away from σ_{χ_1} . Note that by definition for any $(\sigma_3, \sigma_4) \in \Sigma_{34}$, $\sigma_{\chi_3} = \sigma_{\chi_4}$ (and analogously $\sigma_{\chi_1} = \sigma_{\chi_2}$) so the above definition effectively bounds the distance between both chronological components of the label.

Consider the OMTS T_1, T_2, T_3, T_4 , with T_1 in a feedback loop with T_2 , and T_3 with T_4 . Let V_{13} be a τ_{13} -STAS function of T_1 by T_3 (Def. 4.1), and V_{24} be a τ_{24} -STAS function of T_2 by T_4 . All systems share the same label set Σ . We introduce the following functions to keep the equations manageable: given $q'_1 \in Q_1, q_3 \in Q_3, \sigma_i \in \Sigma$, define

$$\begin{aligned} \underline{V}_{13}(q'_1, q_3, \sigma_1) &:= \inf_{q_3 \xrightarrow{\sigma_3 \in B_{\tau_{13}}(\sigma_1)} q'_3} V_{13}(q'_1, q'_3) \\ \underline{V}_{24}(q'_2, q_4, \sigma_2) &:= \inf_{q_4 \xrightarrow{\sigma_4 \in B_{\tau_{24}}(\sigma_2)} q'_4} V_{24}(q'_2, q'_4) \end{aligned}$$

Consider \underline{V}_{13} : if we think of T_3 as trying to match T_1 transitions by minimizing V_{13} over the label ball $B_{\tau_{13}}$, then \underline{V}_{13} measures how well it does it. Similarly for \underline{V}_{24} .

Because STAS functions certify STAS relations via (6), the following theorem provides a way to build STAS functions for interconnections of systems, from the STAS functions of the individual connected systems.

Theorem 4.1: Consider the OMTS T_1, T_2, T_3, T_4 with common label set Σ interconnected as described above. Let V_{13} be a τ_{13} -STAS function of T_1 by T_3 , and V_{24} be a τ_{24} -STAS function of T_2 by T_4 . Set $\tau = \min(\tau_{13}, \tau_{24})$.

Define $V : Q_{12} \times Q_{34} \rightarrow \mathbb{R}_+$ to be $V((q_1, q_2), (q_3, q_4)) = h(V_{13}(q_1, q_3), V_{24}(q_2, q_4))$ where h is continuous and non-decreasing in both arguments.

Recall the definition of lifted label sets Σ_{12}, Σ_{34} in (2). Let $g : \mathbb{R} \rightarrow \mathbb{R}$ be a non-decreasing function s.t. $g(x) \geq x$

and for all $q_{12} \in Q_{12}, q_{34} \in Q_{34}$, g satisfies

$$\begin{aligned} & \sup_{q_{12} \xrightarrow{(\sigma_1, \sigma_2) \in \Sigma \times \Sigma} q'_{12}} h(\underline{V}_{13}(q'_1, q_3, \sigma_1), \underline{V}_{24}(q'_2, q_4, \sigma_2)) \geq \\ & g \left(\sup_{q_{12} \xrightarrow{(\sigma_1, \sigma_2) \in \Sigma_{12}} q'_{12}} h(\underline{V}_{13}(q'_1, q_3, \sigma_1), \underline{V}_{24}(q'_2, q_4, \sigma_2)) \right) \end{aligned} \quad (7)$$

Also, let $\gamma_1, \gamma_2 : \mathbb{R} \rightarrow \mathbb{R}_+$ be continuous non-increasing functions s.t. $\gamma_i(x) \leq x$, $i = 1, 2$, and for all $\sigma_{12} = (\sigma_1, \sigma_2) \in \Sigma_{12}$, for all $(q_3, q_4) \in Q_{34}$, and all $(q'_1, q'_2) \in Q_{12}$

$$\underline{V}_{13}(q'_1, q_3, \sigma_1) \geq \gamma_1 \left(\inf_{q_3 \xrightarrow{B_\tau^{34}(\sigma_{12})} q'_3} V_{13}(q'_1, q'_3) \right) \quad (8)$$

$$\underline{V}_{24}(q'_2, q_4, \sigma_2) \geq \gamma_2 \left(\inf_{q_4 \xrightarrow{B_\tau^{34}(\sigma_{12})} q'_4} V_{24}(q'_2, q'_4) \right) \quad (9)$$

If the following conditions hold:

- (a) V is continuous in the product topology of $Q_{12} \times Q_{34}$.
- (b) For all $q_{12} \in Q_1 \times Q_2, q_{34} \in Q_3 \times Q_4$,

$$V(q_{12}, q_{34}) \geq d_\Pi(\langle q_{12} \rangle, \langle q_{34} \rangle) \quad (10)$$

- (c) Function g distributes over h , that is

$$g(h(x, x')) = h(g(x), g(x')) \quad \forall x, x'$$

- (d) [Small Gain Condition] For all $x \in \mathbb{R}$,

$$g \circ \gamma_1(x) \geq x, \quad g \circ \gamma_2(x) \geq x$$

then V is a τ -STAS function of $T_1 \circ T_2$ by $T_3 \circ T_4$. \square

Before proving the theorem, a few words are in order about its hypotheses. A function g satisfying (7) always exists: by observing that $\Sigma_{12} \subset \Sigma \times \Sigma$, we see that g can be taken to be the identity. A non-identity function quantifies how restrictive is the interconnection $T_1 \circ T_2$. It does so by quantifying the difference between the full label set $\Sigma \times \Sigma$ available to the individual systems operating without interconnection (on the LHS of inequality (7)), and the restricted label set Σ_{12} available to them as part of the interconnection (on the RHS).

Similarly, functions γ_1, γ_2 satisfying (9) always exist: we can take γ_i to be identically zero. These choices, however, are unlikely to be useful: we need γ_i to quantify how restrictive is the interconnection $T_3 \circ T_4$. They do so by quantifying the difference between the full label ball $B_{\tau_{13}}(\sigma_1) \times B_{\tau_{24}}(\sigma_2)$ available to the individual systems operating without interconnection, and the restricted label ball $B_\tau^{34}(\sigma_{12}) \subset B_{\tau_{13}}(\sigma_1) \times B_{\tau_{24}}(\sigma_2)$ available to them as part of the interconnection. See Fig.3 for an illustration of the label sets.

These two aspects are similar to the conditions, in more classical Lyapunov-based small gain theorems, placing a minimum on the rate of decrease of the Lyapunov functions of the individual systems, and that bound is related to the growth of the other system’s Lyapunov function. (For example results on input-to-state stability [11],[21], and for bisimulation functions in non-hybrid systems [6]). Now the

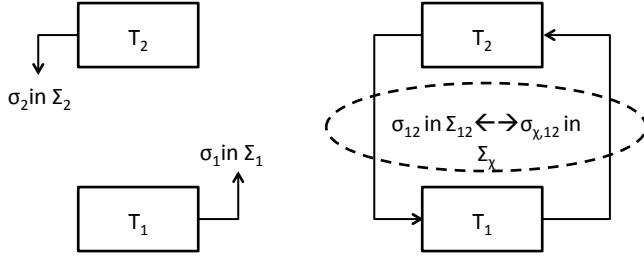


Fig. 3. Label sets constrained by interconnection. Σ_{12} is the set of label pairs compatible with the interconnection as given in Def.2.2.

more restrictive $T_1 \circ T_2$ is, the bigger g can be. The more restrictive $T_3 \circ T_4$ is, the smaller γ_i need to be. The Small Gain Condition (SGC) says that the restrictiveness of $T_1 \circ T_2$ must be balanced by that of $T_3 \circ T_4$: if $T_3 \circ T_4$ is too restrictive ($\gamma_i(x) \ll x$) relative to $T_1 \circ T_2$ ($g \circ \gamma_i(x) < x$), then $T_1 \circ T_2$ can play a label σ_{12} that can't be matched, and thus we lose similarity of the systems. Thus similar to the classical results (e.g., [6]), the SGC balances the gains of the feedback loops.

Proof: (Thm. 4.1)

We seek a STAS function $V : Q_{12} \times Q_{34} \rightarrow \overline{\mathbb{R}}_+$ which would certify that $T_3 \circ T_4$ simulates $T_1 \circ T_2$, and we seek the corresponding precision (τ, ε) .

For notational convenience, introduce

$$\underline{V}(q'_{12}, q_{34}, \sigma_{12}) := \inf_{q_{34} \xrightarrow{\sigma' \in B_\tau^{34}(\sigma_{12})} q'_{34}} V(q'_{12}, q'_{34})$$

By definition, V must satisfy for all $(q_{12}, q_{34}) \in Q_{12} \times Q_{34}$,

$$\text{A0)} \quad V(q_{12}, q_{34}) \geq d_\Pi(\langle q_{12} \rangle, \langle q_{34} \rangle)$$

A1)

$$V(q_{12}, q_{34}) \geq \sup_{q_{12} \xrightarrow{\sigma \in \Sigma_{12}} q'_{12}} \left(\inf_{q_{34} \xrightarrow{\sigma' \in B_\tau^{34}(\sigma)} q'_{34}} V(q'_{12}, q'_{34}) \right)$$

Condition A0 is the same as (10), and so is true by hypothesis. Now for A1. First we restate it using \underline{V} :

$$V(q_{12}, q_{34}) \geq \sup_{q_{12} \xrightarrow{(\sigma_1, \sigma_2) \in \Sigma_{12}} q'_{12}} \underline{V}(q'_{12}, q_{34}, \sigma)$$

For all q_1, q_2, q_3, q_4 ,

$$\begin{aligned} & h(V_{13}(q_1, q_3), V_{24}(q_2, q_4)) \\ & \geq h(\sup_{\Sigma_1} \underline{V}_{13}(q'_1, q_3, \sigma_1), \sup_{\Sigma_2} \underline{V}_{24}(q'_2, q_4, \sigma_2)) \\ & \geq \sup_{\Sigma_1} \sup_{\Sigma_2} h(\underline{V}_{13}(q'_1, q_3, \sigma_1), \underline{V}_{24}(q'_2, q_4, \sigma_2)) \\ & = \sup_{(\sigma_1, \sigma_2) \in \Sigma_1 \times \Sigma_2} h(\underline{V}_{13}(q'_1, q_3, \sigma_1), \underline{V}_{24}(q'_2, q_4, \sigma_2)) \end{aligned}$$

where we used property A1 for V_{13} and V_{24} and the fact that h is non-decreasing to obtain the first inequality, and the non-decreasing nature of h to obtain the second inequality. (The second inequality becomes equality if \underline{V}_{13} and \underline{V}_{24} achieve

their suprema over Σ_1 and Σ_2 respectively.) Using (7), it comes

$$\begin{aligned} & h(V_{13}, V_{24}) \geq \\ & g\left(\sup_{q_{12} \xrightarrow{(\sigma_1, \sigma_2) \in \Sigma_{12}} q'_{12}} h(\underline{V}_{13}(q'_1, q_3, \sigma_1), \underline{V}_{24}(q'_2, q_4, \sigma_2))\right) \end{aligned}$$

Applying (8),(9) to the RHS of this last inequality,

$$\begin{aligned} & h(V_{13}, V_{24}) \geq \\ & g\left(\sup_{q_{12} \xrightarrow{(\sigma_1, \sigma_2) \in \Sigma_{12}} q'_{12}} h(\gamma_1(\inf_{B_\tau^{34}(\sigma_{12})} V_{13}), \gamma_2(\inf_{B_\tau^{34}(\sigma_{12})} V_{24}))\right) \end{aligned}$$

where we are using $\inf_{B_\tau^{34}(\sigma_{12})} V_{ij}$ as an abbreviation for

$$\inf_{q_j \xrightarrow{B_\tau^{34}(\sigma_{12})} q'_j} V_{ij}(q'_i, q'_j)$$

We now establish two inequalities. First, note that

$$\gamma_1(\inf_{B_\tau^{34}(\sigma_{12})} V_{13}) \geq \inf_{B_\tau^{34}(\sigma_{12})} \gamma_1(V_{13}) \quad (11)$$

Indeed, let

$$\bar{Q}_3 = \text{Post}(q_3, B_\tau^{34}(\sigma_{12}))$$

be the set over which the infimization is happening. We have that $v_* := \inf_{B_\tau^{34}(\sigma_{12})} V_{13}(q'_1, q'_3)$ is finite since V is lower bounded by 0. Now since $v_* \leq v$ for all $v \in V_{13}(\bar{Q}_3)$, and γ_1 is non-increasing, it follows that $\gamma_1(v_*) \geq \gamma_1(v)$ for all $v \in V_{13}(\bar{Q}_3)$. Taking the infimum on the RHS, the inequality (11) follows. An inequality analogous to (11) holds for γ_2 by a similar argument.

Second, note that because γ_i and V are continuous, and \bar{Q}_3 is compact, then the set $\gamma_i \circ V(\bar{Q}_3)$ is compact as well. Since h is continuous as well, it achieves its infimum over compact sets and therefore

$$\begin{aligned} & h(\inf_{B_\tau^{34}(\sigma_{12})} \gamma_1(V_{13}), \inf_{B_\tau^{34}(\sigma_{12})} \gamma_2(V_{24})) \\ & = \inf_{B_\tau^{34}(\sigma_{12})} h(\gamma_1 \circ V_{13}, \gamma_2 \circ V_{24}) \end{aligned} \quad (12)$$

We can proceed as

$$\begin{aligned} & h(V_{13}, V_{24}) \\ & \geq g\left(\sup_{q_{12} \xrightarrow{\sigma_{12}} q'_{12}} h(\gamma_1(\inf_{B_\tau^{34}(\sigma_{12})} V_{13}), \gamma_2(\inf_{B_\tau^{34}(\sigma_{12})} V_{24}))\right) \\ & \geq g\left(\sup_{q_{12} \xrightarrow{\sigma_{12}} q'_{12}} h(\inf_{B_\tau^{34}(\sigma_{12})} \gamma_1(V_{13}), \inf_{B_\tau^{34}(\sigma_{12})} \gamma_2(V_{24}))\right) \\ & = g\left(\sup_{q_{12} \xrightarrow{\sigma_{12}} q'_{12}} \inf_{B_\tau^{34}(\sigma_{12})} h(\gamma_1 \circ V_{13}, \gamma_2 \circ V_{24}))\right) \\ & = \sup_{q_{12} \xrightarrow{\sigma_{12}} q'_{12}} \inf_{B_\tau^{34}(\sigma_{12})} g \circ h(\gamma_1 \circ V_{13}, \gamma_2 \circ V_{24}) \end{aligned}$$

To obtain the second inequality, we used (11) and the fact that h and g are non-decreasing. To obtain the equalities, we used (12) and the fact that g is non-decreasing.

By distributivity of g over h and the SGC

$$\begin{aligned}
& h(V_{13}, V_{24}) \\
& \geq \sup_{q_{12} \xrightarrow{\sigma_{12}} q'_{12}} \inf_{B_{\tau}^{34}(\sigma_{12})} h(g \circ \gamma_1 \circ V_{13}, g \circ \gamma_2 \circ V_{24}) \\
& \geq \sup_{q_{12} \xrightarrow{\sigma_{12}} q'_{12}} \inf_{q_{34} \xrightarrow{B_{\tau}^{34}(\sigma_{12})} q'_{34}} h(V_{13}, V_{24})
\end{aligned}$$

thus concluding that $V = h(V_{13}, V_{24})$ satisfies A1, and so is a τ -STAS function. ■

About the other conditions The distributivity assumption in (c) holds, for example, if h is the max operator, i.e. $h(x, x') = \max(x, x')$.

Thm. 4.1 assures us that feedback interconnection respects similarity relation, and therefore also respects conformance relations.

However, the conditions defining g and γ_i (equations (7) and (9),(8)) are technical conditions that are hard to check. Turning them into a computational tool for particular classes of systems is the subject of current research. A simpler, and more conservative, criterion is given in the following theorem:

Theorem 4.2: If

$$k_1 := \frac{\inf_{Q_1} \inf_{Q_3} V_{13}(q_1, q_3)}{\sup_{Q_3} \sup_{Q_1} V_{13}(q_1, q_3)} < \infty$$

then $\gamma_1(v) = k_1 v$ satisfies (8). Similarly, if

$$k_2 := \frac{\inf_{Q_2} \inf_{Q_4} V_{24}(q_2, q_4)}{\sup_{Q_4} \sup_{Q_2} V_{24}(q_2, q_4)} < \infty$$

then $\gamma_2(v) = k_2 v$ satisfies (9). □

Proof: We give the proof for k_1 , that for k_2 is similar. Define $\bar{Q}_3 = \{q'_3 \mid \exists q_3 \xrightarrow{B_{\tau}^{34}(\sigma_{12})} q'_3\}$ and $\hat{Q}_3 = \{q'_3 \mid \exists q_3 \xrightarrow{B_{\tau_{13}}(\sigma_1)} q'_3\}$. Since $\text{pr}_{\Sigma}(B_{\tau}^{34}(\sigma_{12})) \subset B_{\tau_{13}}(\sigma_1)$, $\bar{Q}_3 \subset \hat{Q}_3 \subset Q_3$. Thus for any $q'_1 \in Q_1$

$$\begin{aligned}
& \inf_{q'_3 \in \bar{Q}_3} V_{13}(q'_1, q'_3) \geq \inf_{q'_3 \in \bar{Q}_3} V_{13}(q'_1, q'_3) \\
& \geq \inf_{q'_3 \in \bar{Q}_3} V_{13}(q'_1, q'_3) \frac{\inf_{\bar{Q}_3} V_{13}(q'_1, q'_3)}{\sup_{Q_3} V_{13}(q'_1, q'_3)} \\
& \geq \frac{\inf_{(q_1, q'_3) \in Q_1 \times Q_3} V_{13}(q_1, q'_3)}{\sup_{(q_1, q'_3) \in Q_1 \times Q_3} V_{13}(q_1, q'_3)} \inf_{\bar{Q}_3} V_{13}(q'_1, q'_3) \\
& = k_1 \inf_{q'_3 \in \bar{Q}_3} V_{13}(q'_1, q'_3)
\end{aligned}$$

The challenge with the choice of γ_1 and γ_2 in Thm. 4.2 is that g is now required to always ‘compensate’ for the worst-case behavior to satisfy the SGC. I.e. we need $g(x) \geq x / \max(k_1, k_2)$ for all x . This may lead to a violation of (7).

The next result follows from Thm.4.1, the fact that h is increasing, and [12, Thm. 3.6].

Theorem 4.3: Let $\varepsilon_{13} = \sup_{Q_1^0} \inf_{Q_3^0} V_{13}(q_1, q_3)$ and $\varepsilon_{24} = \sup_{Q_2^0} \inf_{Q_4^0} V_{24}(q_2, q_4)$, so that T_3 ($\tau_{13}, \varepsilon_{13}$)-simulates T_1 , and T_4 ($\tau_{24}, \varepsilon_{24}$)-simulates T_2 . Then $T_3 \circ T_4$ (τ, ε)-simulates $T_1 \circ T_2$ with $\tau = \min(\tau_{13}, \tau_{24}), \varepsilon = h(\varepsilon_{13}, \varepsilon_{24})$.

V. RELATED WORKS

In this paper we understand conformance as a notion that relates *systems*, as done in [22], rather than a system and its specification as done for example in [4]. Most existing works on system conformance, either requires equality of outputs, or does not account for timing differences, as in [15] where an approximate method for verifying formal equivalence between a model and its auto-generated code is presented. The approach to conformance of Hybrid Input/Output Automata in [17] and falls in the domain of nondeterministic abstractions, and a thorough comparison between this notion and ours is given in [16]. The works closest to ours are [12] and [19]. The work [12] defines the STAS relation we used in this paper. The goal in [12] is to define robust approximate synchronization between systems (rather than conformance testing). The refinement relation between systems given in [20] allows different inputs to the two systems. Conformance requires the same input be applied, which is a more stringent requirement. The current theoretical framework also allows a significantly wider class of systems than in [20].

VI. CONCLUSIONS

When a system model goes through multiple design and verification iterations, it is necessary to get a rigorous and quantitative measure of the similarities between the systems. Conformance testing [2] allows us to obtain such a measure, and to automatically transfer formal verification results from a simpler model to a more complex model of the system. In this paper, we extended the reach of conformance testing by developing the sufficient conditions for feedback interconnections of conformant systems to be conformant. As pointed out earlier, these conditions apply to Open Metric Transition Systems, and while this means they are very broadly applicable, they must be specialized to specific classes of dynamical systems. The next step is to compute STAS functions for various classes of dynamical systems, including hybrid systems. This is the subject of current research. In addition, we aim to apply the compositionality theory developed here to problems in source code generation.

REFERENCES

- [1] H. Abbas, B. Hoxha, G. Fainekos, J. V. Deshmukh, J. Kapinski, and K. Ueda. Conformance testing as falsification for cyber-physical systems. Technical Report arXiv:1401.5200, January 2014.
- [2] H. Abbas, H. Mittelman, and G. Fainekos. Formal property verification in a conformance testing framework. In *MEMOCODE*, 2014.
- [3] K. Butts. Presentation: Toyota’s direction. [Online at: http://cmacs.cs.cmu.edu/presentations/verif.csystems/06_KenButts.pdf], 2010.
- [4] T. Dang and T. Nahhal. Coverage-guided test generation for continuous and hybrid systems. *Formal Methods in System Design*, 34(2):183–213, 2009.
- [5] G. Frehse, C. L. Guernic, A. Donze, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler. Spaceex: Scalable verification of hybrid systems. In *Proceedings of the 23d CAV*, 2011.
- [6] A. Girard. A composition theorem for bisimulation functions. Technical Report, 2007.

- [7] A. Girard and G. J. Pappas. Approximate bisimulations for constrained linear systems. In *Proceedings of 44th IEEE Conference on Decision and Control and European Control Conference*, pages 4700–4705, 2005.
- [8] A. Girard and G. J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Trans. Auto. Cont.*, 52(5):782–798, 2007.
- [9] R. Goebel, R. G. SanFelice, and A. R. Teel. *Hybrid Dynamical Systems: modeling, stability and robustness*. Princeton University Press, 2012.
- [10] R. Goebel and A. Teel. Solutions to hybrid inclusions via set and graphical convergence with stability theory applications. *Automatica*, 42(4):573 – 587, 2006.
- [11] Z.-P. Jiang, I. M. Mareels, and Y. Wang. A lyapunov formulation of the nonlinear small-gain theorem for interconnected {ISS} systems. *Automatica*, 32(8):1211 – 1215, 1996.
- [12] A. Julius and G. Pappas. Approximate equivalence and approximate synchronization of metric transition systems. In *Decision and Control, 2006 45th IEEE Conference on*, pages 905–910, Dec 2006.
- [13] A. A. Julius, A. D’Innocenzo, M. D. D. Benedetto, and G. J. Pappas. Approximate equivalence and synchronization of metric transition systems. *Systems and Control Letters*, 58(2):94 – 101, 2009.
- [14] N. Lynch, R. Segala, and F. Vaandrager. Hybrid i/o automata. *Information and Computation*, 185(1):105 – 157, 2003.
- [15] R. Majumdar, I. Saha, K. Ueda, and H. Yazarel. Compositional equivalence checking for models and code of control systems. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, pages 1564–1571, Dec 2013.
- [16] M. Mohaqeqi, M. R. Mousavi, and W. Taha. Conformance testing of cyber-physical systems: A comparative study. *ECEASST*, 70, 2014.
- [17] M. Osch. Hybrid input-output conformance and test generation. In K. Havelund, M. Nunez, G. Rosu, and B. Wolff, editors, *Formal Approaches to Software Testing and Runtime Verification*, volume 4262 of *Lecture Notes in Computer Science*, pages 70–84. Springer Berlin Heidelberg, 2006.
- [18] A. Platzer and J.-D. Quesel. KeYmaera: A hybrid theorem prover for hybrid systems. In A. Armando, P. Baumgartner, and G. Dowek, editors, *International Joint Conference on Automated Reasoning*, volume 5195 of *LNCS*, pages 171–178. Springer, 2008.
- [19] J.-D. Quesel. *Similarity, Logic, and Games: Bridging Modeling Layers of Hybrid Systems*. PhD thesis, Carl Von Ossietzky Universitat Oldenburg, July 2013.
- [20] J.-D. Quesel, M. Fränzle, and W. Damm. Crossing the bridge between similar games. In S. Tripakis and U. Fahrenberg, editors, *9th FORMATS, Aalborg, Denmark, 21-23 September, 2011. Proceedings*, volume 6919 of *LNCS*, pages 160–176. Springer, Sep. 2011.
- [21] R. G. Sanfelice. Input-output-to-state stability tools for hybrid systems and their interconnections. *IEEE Transactions on Automatic Control*, May 2014.
- [22] J.-P. Talpin, P. Guernic, S. Shukla, and R. Gupta. A compositional behavioral modeling framework for embedded system design and conformance checking. *International Journal of Parallel Programming*, 33(6):613–643, 2005.